## UNITED STATES PATENT AND TRADEMARK OFFICE

Inventor: Collins et al.

Serial No: 09/328,726

Filing Date: October 26, 1998

Docket No: 20206-25 (PT-TA 410 (Cont 1))

Group Art Unit: 2766

Examiner: Leaning, J.

For: **"PUBLIC KEY CRYPTOGRAPHIC APPARATUS AND METHOD"**

Assistant Commissioner for Patents
Washington, D.C. 20231

### AMENDMENT

Sir:

In response to the Office Action mailed on April 27, 2000, Applicants respectfully request reconsideration of the above-identified patent application. Please amend the above identified application as follows and consider the following remarks.

**In the Specification:**

On page 3, line 33, replace "$C = M^e \pmod n$" with --$C \equiv M^e \pmod n$--.

On page 4, line 4, replace "$M = C^d \pmod n$" with --$M \equiv C^d \pmod n$--.

On page 4, line 12, replace "$d = e^{-1} \bmod (p-1)(q-1)$" with --$d \equiv e^{-1} \bmod ((p-1)(q-1))$--.

On page 4, line 8 replace "$e \cdot d = 1(\bmod(\mathrm{lcm}((p-1), (q-1))))$" with --$e \cdot d \equiv 1(\bmod(\mathrm{lcm}((p-1), (q-1))))$--.

On page 8, line 8, replace "$C = M^e \pmod n$" with --$C \equiv M^e \pmod n$--.

On page 8, line 12, replace "$M = C^d \pmod n$" with --$M \equiv C^d \pmod n$--.

On page 8, line 17, replace "encryption" with --decryption--.

On page 9, line 21, between "each" and "is", insert --of $(p_1-1)$, $(p_2-1)$, ..., $(p_k-1)$--.

On page 9, line 26, replace "$d = e^{-1} \bmod ((p_1-1) (p_2-1) \ldots (p_k-1))$." with --$d \equiv e^{-1} \bmod ((p_1-1) (p_2-1) \ldots (p_k-1))$.--

On page 9, line 29, replace "$C = M^e \bmod n$" with --$C \equiv M^e \pmod n$--.

On page 9, lines 28-29, replace "using the relationship of (3), above, i.e.," with --using relationship (3), reprinted below.--

-1-